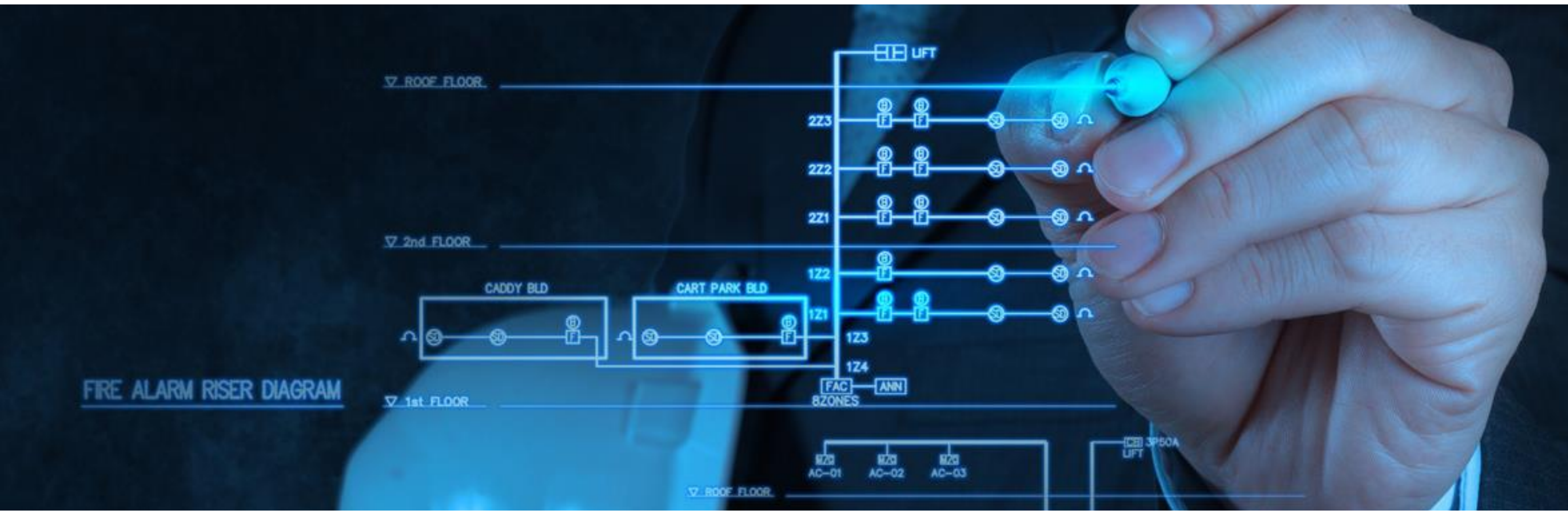
G. Bina

Secure Your Cyber-Space & IT



Securing Industrial Control Systems (ICS)

A 3 day learning program which Include demonstrations of the Israeli security management state of the art methodologies

Developed by Dr. Col. (res.) Gabi Siboni

Securing Industrial Control Systems (ICS)

A 3 day Seminar

Introduction

AS Control systems are widely and commonly deployed and ICS incidents frequency is increasing, securing industrial control systems is becoming more and more critical. This mission needs special attention as it requires to integrate the knowledge of security professionals and control system engineers and to develop a unique expertise.

About the Course Owner and Developer

This course is developed by Dr. Col. (res.) Gabi Siboni, Director of The Cyber Security Program at The Institute for National Security Studies, Tel Aviv University and Serves as chief methodologist of the IDF's Research Center for Force Utilization and Buildup – Experimentation Laboratory.

Dr. Siboni is a domain expert in national security, military strategy and operations, military technology, cyber security and warfare, and force buildup and a thought leader in business operations risk management.

Who Should Attend?

Information security managers, software developers, CIOs and CISOs who are seeking for a full spectrum understanding of the ICS arena and securing ICS and for those who seek to develop a core competence in this filed.

Course Curriculum

This training is designed to present and demonstrate the most up-to-date knowledge-base methodologies, technologies and techniques needed to ensure a secure automation and control system. The lectures and examples will focus on the state of the art Israeli expertise in protecting ICS across different arenas including the defense sector.

Topic	Contents
Introduction to Industry Control Systems	Overview of ICS, Field components, network components, communications, ICS application overview, industry models
ICS Attack Surface	Overview of ICS attack surface, attacks on HMIs, attacks on control servers, attacks on network communications, attacks on remote devices
Defending ICS Servers and Workstations	ICS server and workstation technologies, ICS server operating systems, enforcing security policy, ICS hardening
Defending ICS Networks and Devices	Firewalls and honeypots, wireless network security, controller and field device security, cryptography fundamentals
ISC Risk Management	Risk and manufacturing systems, threat identification, vulnerability management, industrial consequences, risk classification and risk reduction
ICS Auditing, ICS Contingency and Continuity Planning	Vulnerability assessment and auditing, Business Impact Analysis (BIA) and Business Continuity Plan (BCP), Developing crisis strategy
ICS Applied Security	Standards and security controls, understanding and using ICS security technologies, physical security

* * Learning materials will be provided to participants by a magnetic means